IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of:	§	
	§	
	§	
U.S. Patent Number 5,623,600	§	Control No.: Not Yet Assigned
	§	
Issued: April 22, 1997	§	Group Art Unit: Not Yet Assigned
	§	
For: Virus Detection and Removal for	§	Examiner: Not Yet Assigned
Computer Networks	§	
	§	Attorney Docket No.: FORT-000013L

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLACEMENT STATEMENT AND EXPLANATION UNDER 37 C.F.R. § 1.510(b)(1) and (2) TO PREVIOUSLY SUBMITTED REQUEST FOR *EX PARTE* REEXAMINATION UNDER 35 U.S.C. §§ 302-307

Dear Sir:

In response to the "Notice of Failure to Comply with *Ex Parte* Reexamination Request Filing Requirements" mailed June 21, 2010 ("**Notice**") in connection with the above-captioned Request for *Ex Parte* Reexamination submitted June 1, 2010 ("**Request**"), Fortinet, Inc. ("**Fortinet**" or "**Requestor**"), by and through its undersigned attorneys respectfully submits the following Replacement Statement and Explanation Under 37 C.F.R. § 1.510(b)(1) and (2) ("**Replacement Statement and Explanation**") in place of the originally-filed statement and explanation of Sections V and VI of the Request.

Responsive to the indication in the Notice that the "explanation must not [] lump together the proposed rejections or proposed combinations of references," below, the Requestor has now limited the explanations to those explicitly recited prior art combinations expressed by the substantial new questions (SNQs) of patentability.

Please replace the originally-filed statement and explanation with the Replacement Statement and Explanation of Sections V and VI provided immediately below:

V. STATEMENT UNDER 37 C.F.R. § 1.510(B)(1) OF EACH SUBSTANTIAL NEW QUESTION OF PATENTABILITY BASED UPON PREVIOUSLY UNCITED PRIOR ART, INCLUDING DETAILED EXPLANATIONS FOR PERTINENCE AND MANNER OF APPLYING PRIOR ART UNDER 35 U.S.C. § 103

The claims of the '600 patent are unpatentable under 35 U.S.C. §103(a) in view of the prior art references provided herewith, which were not previously presented during the examination of the patent. As the following discussion demonstrates, claims 1-22 (all of the claims) of the '600 patent are invalid under 35 U.S.C. § 103(a) in view of the previously uncited prior art references under any reasonable interpretation of the claims.

The following is a list of each substantial new question of patentability based on prior patents and printed publications pursuant to 37 C.F.R. § 1.510(b)(1). References below are to claims in the '600 patent.

A. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of LANProtect;

B. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of TIS Firewall;

C. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of TFS Manual;

D. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of MIMEsweeper;

E. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper, and further in view of Hile;

F. Whether claim 2 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect and TIS Firewall, and further in view of Hile;

G. Whether claim 3 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper, and further in view of Hile;

H. Whether claim 4 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of TIS Firewall, and further in view of Sidewinder;

I. Whether claim 4 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall, and further in view of TFS Manual;

J. Whether claim 5 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect;

K. Whether claim 5 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall in view of Sidewinder, and further in view of MIMEsweeper;

L. Whether claim 6 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall;

M. Whether claim 6 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan;

N. Whether claim 7 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TFS Manual;

O. Whether claim 7 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of TIS Firewall;

P. Whether claim 8 unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TFS Manual;

Q. Whether claim 8 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MIMEsweeper;

R. Whether claim 9 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall;

S. Whether claim 9 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of Sidewinder;

T. Whether claim 10 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall;

U. Whether claim 10 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of Sidewinder;

V. Whether claim 11 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

W. Whether claim 11 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper and Sidewinder, and further in view of MpScan;

X. Whether claim 12 is unpatentable under 35 U.S.C. § 103 as being obvious over MpScan in view of MIMEsweeper;

Y. Whether claim 13 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

Z. Whether claim 13 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin and TIS Firewall, and further in view of TFS Manual;

AA. Whether claim 14 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

BB. Whether claim 14 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, TIS Firewall, Sidewinder, MpScan and Layland, and further in view of Hile;

CC. Whether claim 15 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall;

DD. Whether claim 15 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan;

EE. Whether claim 16 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

FF. Whether claim 16 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100;

GG. Whether claim 17 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

HH. Whether claim 17 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100;

II. Whether claim 18 unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect, Cheswick and Bellovin and TIS Firewall, and further in view of Hile;

JJ. Whether claim 19 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall;

KK. Whether claim 19 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan;

LL. Whether claim 20 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper;

MM. Whether claim 20 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect, MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100;

NN. Whether claim 21 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect;

OO. Whether claim 21 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect, and further in view of Sidewinder;

PP. Whether claim 22 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect and MIMEsweeper, and further in view of Cheswick and Bellovin; and

QQ. Whether claim 22 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect, MIMEsweeper, Cheswick and Bellovin and MpScan, and further in view of TIS Firewall.

VI. PERTINENCE AND MANNER OF APPLYING PRIOR ART UNDER 35 U.S.C. § 103

Claims 1-22 of the ‘600 patent are obvious in view of the proposed combinations of Cheswick, Cheswick and Bellovin, Layland, LANProtect, Sidewinder, TIS Firewall, Hile, TFS Manual, MIMEsweeper, MpScan and SunScreen SPF-100 as described further below.

General Motivation to Combine

Because all of the prior art presented herewith was well known and readily at hand to both applicant and similar security industry participants, under the articulated KSR obviousness standard[1],all of these highly relevant and related teachings and technology relating to virus scanning contained in Cheswick, Cheswick and Bellovin, Layland, LANProtect, Sidewinder, TIS Firewall, TFS Manual, MIMEsweeper, MpScan and SunScreen SPF-100 and Hile are properly combinable and are representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of virus detection. Indeed, various of these references explicitly cite or refer to other of these references. For example, Cheswick and Bellovin includes an express discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and SunScreen SPF-100 cites to Cheskwick and Bellovin (see, e.g., SunScreen SPF-100 at pg. 30) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

[1] In KSR International Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007), the Supreme Court “beg[a]n by rejecting the rigid approach of the Court of Appeals” (i.e., requiring satisfaction of the “teaching, suggestion, motivation” (TSM) test) to show an invention would have been obvious (and is therefore unpatentable). Returning to its own nonobviousness cases, the Court held that “the [nonobviousness] analysis **need not seek out precise teachings directed to the *specific subject matter* of the challenged claim**, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.”

The discussion below presents the pertinence and manner of applying the prior art under 35 U.S.C. § 103(a). The references are to the respective claims, Claims 1-22, in the '600 patent.

A. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin and further in view of LANProtect

None of Cheswick, Cheswick and Bellovin and LANProtect were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the '600 patent, which elements were mistakenly considered points of novelty by the Examiner in allowing such claims.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,….. the memory including a server for scanning data for a virus..

- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin and LANProtect together disclose (either expressly or inherently) and render obvious each limitation of claim 1. A more detailed element-by-element analysis is presented below.

Cheswick was not considered during the prosecution of the ‘600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T’s secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T’s internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick describes implementations of network systems utilizing firewall and gateways. Cheswick evidences the fact that proxies and daemons are rudimentary building blocks of firewalls and gateways and firewalls and gateways routinely and customarily implement proxy servers. Cheswick also describes the use of daemons in scanning services. See e.g., Cheswick at

234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick and Bellovin was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers and daemons within firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect also describes the claimed aspect of using a proxy server in connection with scanning for viruses at a gateway. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect."). At the time of its release, more than three years prior to the filing date of the '600 patent, LANProtect was recognized by the National Computer Security Association (NCSA) as "an entirely new category of product … that shifts the virus protection paradigm … to server-based protection." See, LANProtect at pg. 1.

LANProtect includes proxy servers by virtue of the fact that it runs in concert with the Netware operating system, and by virtue of its LProtect module. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses."). As noted earlier, LANProtect was jointly developed and marketed by Intel and Trend Micro; therefore, Trend Micro knew or should have known at least some of the reasons for allowance identified during the original examination of the '600 patent were flawed (i.e., the recitation by certain claims of a proxy server and/or a daemon).

The teachings relating to use of a proxy server and a daemon in connection with removing a virus during data transfers as contained in these references as presented in detail below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

Claim 1: "A system for"

(1) "...detecting and selectively removing viruses in data transfers..."

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70.

Importantly, Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect teaches the use and construction of a network server that can detect and handle viruses in data transfers. See LANProtect at 1 ("Intel has taken a unique approach [with LANProtect], implementing virus protection as a network service rather than as a network application. Intel has done so by basing LANProtect on a network architecture that ***provides protection at the server*** without impacting performance—an architecture that will become the model for network-based virus protection in the future." Emphasis Added.); and LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

(2) "…a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. See LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

(3) "…a communications unit for receiving and sending data in response to control signals..."

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect necessarily includes communications units to send and receive data in response to control signals as indicated by this element. LANProtect discusses handling network traffic, which is comprised of various network protocols, such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

(4) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and

Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning.

(5) "…a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a "proxy server" can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect includes proxy servers by virtue of the fact that it runs in concert with the Netware operating system, and by virtue of its LProtect module. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect.").

(6) "…a daemon for transferring data from the proxy server in response to control signals from the proxy server…"

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the '600 patent was filed.

"Daemons" are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the '600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses and describes network communications systems, which when implemented as disclosed, necessarily have communications units to send and receive data as indicated by this element. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers.

None of Cheswick, Cheswick and Bellovin and LANProtect were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. No prior art considered during prosecution of the '600 patent was suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers as documented by Cheswick, Cheswick and Bellovin and LANProtect. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 1 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by LANProtect in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin and LANProtect are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

B. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of TIS Firewall

None of Cheswick, Cheswick and Bellovin and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,..... the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin and TIS Firewall together disclose (either expressly or inherently) and render obvious each limitation of claim 1. A more detailed element-by-element analysis is presented below.

Cheswick was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick describes implementations of network systems utilizing firewall and gateways. Firewalls and gateways routinely and customarily implement proxy servers. It also mentions the use of daemons in scanning services. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick and Bellovin was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin describes firewalls and gateways routinely and customarily implement proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. TIS Firewall specifically and clearly discloses the use of an

FTP/SMTP daemon for ensuring secure connection across different networks. See TIS Firewall at 10 ("The toolkit includes source code for a modified version of the ***FTP daemon*** which permits an administrator to provide both FTP service and FTP proxy service on the same system." Emphasis added.) See also, TIS Firewall at pg. 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security ***an FTP proxy server is provided***." Emphasis added.) See also, TIS Firewall at pg. 4 ("***The toolkit software provides proxy services*** for common applications like FTP and TELNET, and security for SMTP mail." Emphasis added.)

The teachings as contained in Cheswick, Cheswick and Bellovin and TIS Firewall were not present during the prior examination of the '600 patent. For this reason, the teachings of Cheswick, Cheswick and Bellovin and TIS Firewall raise a substantial new question of patentability with respect to at least claim 1 of the '600 patent.

The teachings relating to use of a proxy server and a daemon in connection with removing a virus during data transfers as contained in the references presented below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

Claim 1: "A system for"

(1) "...detecting and selectively removing viruses in data transfers..."

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70.

Importantly, Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall discloses an application-level firewall. As part of transferring messages, it checked for the presence of specific message features that were associated with known worms. Cheswick and Bellovin note that the TIS Firewall Toolkit can monitor incoming SMTP traffic, and "provides a hook for any necessary prefiltering of letter bombs." Cheswick and Bellovin at pg. 115. TIS Firewall also checked for the presence of certain keywords in the message. As scanning for keywords representative of harmful content is equivalent to scanning for viruses, this element is taught by TIS Firewall.

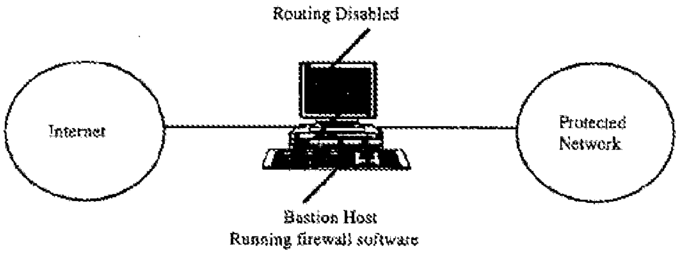
(2) "…a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. The Bastion host (see figure below) that runs the firewall software necessarily has a memory unit and any person skilled in the art would recognize the memory as an inherent feature of the TIS Firewall.



(3) "...a communications unit for receiving and sending data in response to control signals..."

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall discloses a firewall system that provides secure access to the outside network. A firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

(4) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall discloses a firewall system that provides a secure access to the outside network. A Firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art. The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

(5) "…a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a "proxy server" can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, TIS Firewall discloses a firewall system that handled SMTP and FTP traffic and acts as a proxy server. See TIS Firewall at 4 ("The toolkit software provides proxy services for common applications like FTP and TELNET, and security for SMTP mail. Since the bastion host is a security-critical network strong point, it is important that the configuration of the software on that system be as secure as possible.")

(6) "…a daemon for transferring data from the proxy server in response to control signals from the proxy server…"

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the ‘600 patent was filed.

“Daemons” are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the ‘600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 (“Gateway tools”, discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall discloses a firewall system for secure connection across different networks.

TIS firewall uses an SMTP/FTP daemon. The FTP daemon in TIS Firewall was used to handle FTP communication. See TIS Firewall at 10 ("The toolkit includes source code for a modified version of the FTP daemon which permits an administrator to provide both FTP service and FTP proxy service on the same system.")

None of Cheswick, Cheswick and Bellovin and TIS Firewall were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. No prior art considered during prosecution of the '600 patent was suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers as documented by Cheswick, Cheswick and Bellovin and TIS Firewall. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 1 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by TIS Firewall in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin and TIS Firewall are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

C. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of TFS Manual

None of Cheswick, Cheswick and Bellovin and TFS manual were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,..... the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious. Hile, which was considered during the prosecution of the '600 patent, discloses these elements as detailed below.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin and TFS manual together disclose (either expressly or inherently) and render obvious each limitation of claim 1. A more detailed element-by-element analysis is presented below.

Cheswick was not considered during the prosecution of the ‘600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T’s secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T’s internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick describes implementations of network systems utilizing firewall and gateways. Firewalls and gateways routinely and customarily implement proxy servers. It also mentions the use of daemons in scanning services. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick and Bellovin was not considered during prosecution of the ‘600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin describe firewalls and gateways routinely and customarily implement proxy servers. See Cheswick and Bellovin at Chapter 6 (“Gateway tools”, discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

TFS Manual was not considered during the prosecution of the ‘600 patent. It was published in 1995, to discuss data transfer across different networks. TFS manual discloses a proxy server in context of email transfers. Here, the proxy server handles SMTP traffic. See TFS Manual at 37 (“A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME."). In order to process SMTP connections, it is well-known to insert SMTP proxies on the incoming network for anti-spam and anti-virus techniques.

The teachings as contained in Cheswick, Cheswick and Bellovin and TFS manual were not present during the prior examination of the '600 patent. For this reason, the teachings by Cheswick, Cheswick and Bellovin and TFS manual raise a substantial new question of patentability with respect to at least claim 1 of the '600 patent.

The teachings relating to use of a proxy server and a daemon in connection with removing a virus during data transfers as contained in the references presented below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

Claim 1: "A system for"

(1) "...detecting and selectively removing viruses in data transfers..."

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70.

Importantly, Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TFS Manual discloses a method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems.") and TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

(2) "…a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, the TFS Gateway as described by the TFS Manual has memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and the recipient will be notified. Requirements: To use this feature you need a Virus program, e.g. Dr Salomon's Antivirus.")

(3) "…a communications unit for receiving and sending data in response to control signals..."

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TFS Manual discloses a series of gateway products that acts as a link between local as well as global mail systems. A gateway system as disclosed in the TFS Manual necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

(4) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TFS Manual discloses and describes a gateway system, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in this system, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning. Meanwhile, it is inherent and common sense to make a decision based on a check being performed. Therefore, in view of the fact that TFS Manual expressly teaches checking for viruses in all incoming attachments, common sense suggests attachments confirmed to have a virus would not be forwarded to the intended destination and that attachments confirmed not to have a virus would be safe to pass. See TFS Manual at pg. 77.

(5) "…a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a "proxy server" can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TFS Manual discloses a gateway system that handled SMTP traffic and acts as a proxy server. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.") Virtually all manually generated Internet e-mail is transmitted via SMTP in MIME format.

(6) "…a daemon for transferring data from the proxy server in response to control signals from the proxy server…"

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the '600 patent was filed.

"Daemons" are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the '600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TFS Manual discloses a gateway system for sending and receiving e-mail messages across different networks. The TFS gateway uses an SMTP daemon. The SMTP daemon in the TFS Gateway was used to handle SMTP communication, both sending and receiving e-mail messages, including receiving the TCP/IP information and translating it into text files and then taking these files and translating them out to the recipient node. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.")

None of Cheswick, Cheswick and Bellovin and TFS Manual were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. No prior art considered during prosecution of the '600 patent was suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers as documented by Cheswick, Cheswick and Bellovin and TFS Manual. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 1 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by TFS Manual in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin and TFS Manual are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

D. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, and further in view of MIMEsweeper

None of Cheswick, Cheswick and Bellovin and MIMEsweeper were considered during prosecution of the ‘600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the ‘600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the ‘600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,….. the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious. Hile, which was considered during the prosecution of the '600 patent, discloses these elements as detailed below.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin and MIMEsweeper together disclose (either expressly or inherently) and render obvious each limitation of claim 1. A more detailed element-by-element analysis is presented below.

Cheswick was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick describes implementations of network systems utilizing firewall and gateways. Firewalls and gateways routinely and customarily implement proxy servers. It also mentions the use of daemons in scanning services. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick and Bellovin was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin describes firewalls and gateways routinely and customarily implement proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper discloses a proxy server and daemon in the context of mail gateway system that handled SMTP traffic. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation."). MIMEsweeper utilizes a ***daemon*** (e.g., a background process) that is used to handle mail communication. See MIMEsweeper at 75 ("A ***transfer agent*** moves data between message stores, normally without examining or modifying it." Emphasis added. See MIMEsweeper at 13 ("The MIMEsweeper ***SMTP server*** consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent." Emphasis added.)

The teachings as contained in Cheswick, Cheswick and Bellovin and MIMEsweeper were not present during the prior examination of the '600 patent. For this reason, the teachings by Cheswick, Cheswick and Bellovin and MIMEsweeper raise a substantial new question of patentability with respect to at least claim 1 of the '600 patent.

The teachings relating to use of a proxy server and a daemon in connection with removing a virus during data transfers as contained in the references presented below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

Claim 1: "A system for"

(1) "...detecting and selectively removing viruses in data transfers..."

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70.

Importantly, Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper sits between organisations' mail systems, whether internal or external, and scans the contents of all mail for any undesirable attributes. See MIMEsweeper at 10. ("MIMEsweeper was conceived out of a requirement to scan incoming Email attachments for computer viruses").

(2) "…a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. See MIMEsweeper at 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery."); MIMEsweeper at 7 ("Any mail message found to contain a virus … is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified filetypes.") and MIMEsweeper at 9 ("Once in quarantine, MIMEsweeper provides a management tool for … [r]eleasing messages … [d]eletion of messages … [c]opying of quarantined messages … [a]rchiving of MIMEsweeper log files").

(3) "…a communications unit for receiving and sending data in response to control signals..."

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. A mail gateway system as disclosed in MIMEsweeper necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

(4) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

(5) "…a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a "proxy server" can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper discloses a mail gateway system that handled SMTP traffic and incorporates the features of a proxy server. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation.")

(6) "…a daemon for transferring data from the proxy server in response to control signals from the proxy server…"

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the '600 patent was filed.

"Daemons" are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the '600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, MIMEsweeper discloses an email gateway system for secure mail exchange across networks. MIMEsweeper utilizes a daemon that is used to handle mail communication. See MIMEsweeper at 75 ("A transfer agent moves data between message stores, normally without examining or modifying it"). See MIMEsweeper at 13 ("The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.").

None of Cheswick, Cheswick and Bellovin and MIMEsweeper were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. No prior art considered during prosecution of the '600 patent was suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers as documented by Cheswick, Cheswick and Bellovin and MIMEsweeper. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 1 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by MIMEsweeper in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

E. Whether claim 1 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect, TIS Firewall and TFS Manual and MIMEsweeper, and further in view of Hile

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual, and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,….. the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious. <u>Hile</u>, which was considered during the prosecution of the '600 patent, discloses these elements as detailed below.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual and MIMEsweeper together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 1. A more detailed element-by-element analysis is presented below.

Cheswick was not considered during the prosecution of the ‘600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T’s secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T’s internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick describes implementations of network systems utilizing firewall and gateways. Firewalls and gateways routinely and customarily implement proxy servers. It also mentions the use of daemons in scanning services. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick and Bellovin was not considered during prosecution of the ‘600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin describes firewalls and gateways routinely and customarily implement proxy servers. See Cheswick and Bellovin at Chapter 6 (“Gateway tools”, discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

LANProtect was not considered during the prosecution of the ‘600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect also describes the claimed aspect of using a proxy server in connection with scanning for viruses at the gateway. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect.").

TFS Manual was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss data transfer across different networks. TFS manual discloses a proxy server in context of email transfers. Here, the proxy server handles SMTP traffic. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.")

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. TIS Firewall specifically and clearly discloses the use of an FTP/SMTP daemon for ensuring secure connection across different networks. See TIS Firewall at

10 ("The toolkit includes source code for a modified version of the FTP daemon which permits an administrator to provide both FTP service and FTP proxy service on the same system.")

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper discloses a mail gateway system that handled SMTP traffic and incorporates the feature of a proxy server. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation."). MIMEsweeper utilizes a daemon that is used to handle mail communication. See MIMEsweeper at 75 ("A transfer agent moves data between message stores, normally without examining or modifying it"). See MIMEsweeper at 13 ("The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.").

Hile describes an improvement to a personal computer data transfer program that scans data for computer viruses during the data transfer "on the fly" and before the data is stored on a destination storage medium so as to prevent computer viruses from infecting the computer. Hile then automatically inhibits virus-infected data from being stored.[2]

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual and MIMEsweeper were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile (e.g., improvements to a personal computer data transfer program that (i) scans data for computer viruses during the data transfer "on the fly" and before the data is stored on a destination storage medium

[2] Hile at col. 1, ll. 55-62

so as to prevent computer viruses from infecting the computer and (ii) automatically inhibits virus-infected data from being stored) in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 1 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual and MIMEsweeper raise a substantial new question of patentability with respect to at least claim 1 of the '600 patent.

The teachings relating to use of a proxy server and a daemon in connection with removing a virus during data transfers as contained in the references presented below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

Claim 1: "A system for"

(7) "...detecting and selectively removing viruses in data transfers..."

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect teaches the use and construction of a network server that can detect and handle viruses in data transfers. See LANProtect at 1 ("Intel has taken a unique approach [with LANProtect], implementing virus protection as a network service rather than as a network application. Intel has done so by basing LANProtect on a network architecture that ***provides protection at the server*** without impacting performance—an architecture that will become the model for network-based virus protection in the future." Emphasis Added.); and LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TFS Manual discloses a method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems.") and TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses an application-level firewall. As part of transferring messages, it checked for the presence of specific message features that were associated with known worms. Cheswick and Bellovin note that the TIS Firewall Toolkit can monitor incoming SMTP traffic, and "provides a hook for any necessary prefiltering of letter bombs." Cheswick and Bellovin at pg. 115. TIS Firewall also checked for the presence of certain keywords in the message. As scanning for keywords representative of harmful content is equivalent to scanning for viruses, this element is taught by TIS Firewall.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper sits between organisations' mail systems, whether internal or external, and scans the contents of all mail for any undesirable attributes. See MIMEsweeper at 10. ("MIMEsweeper was conceived out of a requirement to scan incoming Email attachments for computer viruses").

(8) "…a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

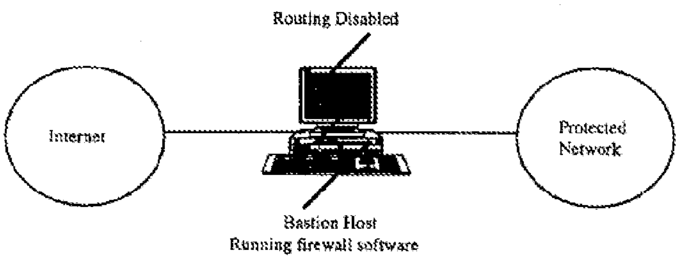
Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. See LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, the TFS Gateway as described by the TFS Manual has memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and the recipient will be notified. Requirements: To use this feature you need a Virus program, e.g. Dr Salomon's Antivirus.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. The Bastion host (see figure below) that runs the firewall software necessarily has a memory unit and any person skilled in the art would recognize the memory as an inherent feature of the TIS Firewall.



In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. See MIMEsweeper at 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery."); MIMEsweeper at 7 ("Any mail message found to contain a virus … is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified filetypes.") and MIMEsweeper at 9 ("Once in quarantine, MIMEsweeper provides a management tool for … [r]eleasing messages … [d]eletion of messages … [c]opying of quarantined messages … [a]rchiving of MIMEsweeper log files").

(9) "…a communications unit for receiving and sending data in response to control signals..."

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect necessarily includes communications units to send and receive data in response to control signals as indicated by this element. LANProtect discusses handling network traffic, which is comprised of various network protocols, such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TFS Manual discloses a series of gateway products that acts as a link between local as well as global mail systems. A gateway system as disclosed in the TFS Manual necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses a firewall system that provides secure access to the outside network. A firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. A mail gateway system as disclosed in MIMEsweeper necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

(10) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TFS Manual discloses and describes a gateway system, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in this system, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning. Meanwhile, it is inherent and common sense to make a decision based on a check being performed. Therefore, in view of the fact that TFS Manual expressly teaches checking for viruses in all incoming attachments, common sense suggests attachments confirmed to have a virus would not be forwarded to the intended destination and that attachments confirmed not to have a virus would be safe to pass. See TFS Manual at pg. 77.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses a firewall system that provides a secure access to the outside network. A Firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art. The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

(11) "…a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a "proxy server" can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect includes proxy servers by virtue of the fact that it runs in concert with the Netware operating system, and by virtue of its LProtect module. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect.").

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TFS Manual discloses a gateway system that handled SMTP traffic and acts as a proxy server. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.") Virtually all manually generated Internet e-mail is transmitted via SMTP in MIME format.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses a firewall system that handled SMTP and FTP traffic and acts as a proxy server. See TIS Firewall at 4 ("The toolkit software provides proxy services for common applications like FTP and TELNET, and security for SMTP mail. Since the bastion host is a security-critical network strong point, it is important that the configuration of the software on that system be as secure as possible.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper discloses a mail gateway system that handled SMTP traffic and incorporates the features of a proxy server. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation.")

(12) "…a daemon for transferring data from the proxy server in response to control signals from the proxy server…"

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the '600 patent was filed.

"Daemons" are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the '600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect discloses and describes network communications systems, which when implemented as disclosed, necessarily have communications units to send and receive data as indicated by this element. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TFS Manual discloses a gateway system for sending and receiving e-mail messages across different networks. The TFS gateway uses an SMTP daemon. The SMTP daemon in the TFS Gateway was used to handle SMTP communication, both sending and receiving e-mail messages, including receiving the TCP/IP information and translating it into text files and then taking these files and translating them out to the recipient node. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TFS Manual, TIS Firewall discloses a firewall system for secure connection across different networks. TIS firewall uses an SMTP/FTP daemon. The FTP daemon in TIS Firewall was used to handle FTP communication. See TIS Firewall at 10 ("The toolkit includes source code for a modified version of the FTP daemon which permits an administrator to provide both FTP service and FTP proxy service on the same system.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TFS Manual and TIS Firewall, MIMEsweeper discloses an email gateway system for secure mail exchange across networks. MIMEsweeper utilizes a daemon that is used to handle mail communication. See MIMEsweeper at 75 ("A transfer agent moves data between message stores, normally without examining or modifying it"). See MIMEsweeper at 13 ("The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.").

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teachings specifically not present during the prosecution of the

‘600 patent. No prior art considered during prosecution of the ‘600 patent was suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers as documented by Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 (“It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.”) And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 1 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by LANProtect, TIS Firewall, TFS Manual, MIMEsweeper and Hile in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual, MIMEsweeper and

Hile are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

F. Whether claim 2 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect and TIS Firewall, and further in view of Hile

None of Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the daemon is an FTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the daemon is an FTP daemon, raise a substantial new question of patentability with respect to claim 2 as pointed out in more detail below.

Claim 2 recites "the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

In total, Claim 2 adds as the specific proxy server type, "a FTP proxy server". However, the restriction on the proxy server element to an FTP proxy server is a meaningless restriction because the FTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every file server and electronic mail system as of the Critical Date.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 2.

Cheswick was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick discloses the use of an FTP proxy server. See Cheswick at 234 ("*Pftp* provides FTP access in a similar manner." "We provide incoming login and mail service. For incoming file transfer, inet provides an anonymous FTP service").

Cheswick and Bellovin was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin also discloses the use of an FTP proxy server. See e.g., Firewalls and Internet Security, Cheswick and Bellovin (1994) at 94 ("As we have described, outgoing FTP sessions normally require an incoming TCP call. To support this, our proxy service can listen on a newly created socket. The port number is passed back to the caller, which generates the appropriate FTP PORT command. The call is thus outgoing from the user's machine to the firewall, but incoming from the FTP server.").

Furthermore, it would have been obvious to use LANProtect at an FTP proxy server and to utilize an FTP daemon. LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect was designed to be installed and run on a NetWare server, which is a computer that has a Novell loadable module running on it. The NetWare server receives a request from a user on the local area network. The NetWare server then determines whether to send the requested information to the user. If the NetWare server decides to send the information to the user, the file is transmitted electronically in units called packets. Each packet includes a header, and part of the information included in the header is the destination address where the information is being sent. See LANProtect at 5 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail me transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses."). In addition, it would have been obvious to use the network file server/scanning system disclosed by the LANProtect at a mail server, and implementing an FTP proxy server and an FTP daemon.

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate

the building of network firewalls. TIS Firewall utilizes an FTP proxy server that handles evaluation and transfer of data files and an FTP daemon that communicates with a recipient node and transfers data to the recipient node. See TIS Firewall at 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security an FTP proxy server is provided.")

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 2 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall raise a substantial new question of patentability with respect to at least claim 2 of the '600 patent.

Claim 2 adds as the specific proxy server type, "a FTP proxy server". However, the restriction on the proxy server element to an FTP proxy server is a meaningless restriction because the FTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every file server and electronic mail system as of the Critical Date.

Claim 2: "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files"

Claim 2 recites "The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

Cheswick discloses the use of an FTP proxy server. See Cheswick at 234 ("*Pftp* provides FTP access in a similar manner." "We provide incoming login and mail service. For incoming file transfer, inet provides an anonymous FTP service").

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discloses the use of an FTP proxy server. See e.g., Firewalls and Internet Security, Cheswick and Bellovin (1994) at 94 ("As we have described, outgoing FTP sessions normally require an incoming TCP call. To support this, our proxy service can listen on a newly created socket. The port number is passed back to the caller, which generates the appropriate FTP PORT command. The call is thus outgoing from the user's machine to the firewall, but incoming from the FTP server.").

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, TIS Firewall utilizes an FTP proxy server that handles evaluation and transfer of data files and an FTP daemon that communicates with a recipient node and transfers data to the recipient node. See TIS Firewall at 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security an FTP proxy server is provided.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and TIS Firewall, it would have been obvious to use the LANProtect at an FTP proxy server and to utilize an FTP daemon. LANProtect was designed to be installed and run on a NetWare server, which is a computer that has a Novell loadable module running on it. The NetWare server receives a request from a user on the local area network. The NetWare server then determines whether to send the requested information to the user. If the NetWare server decides to send the information to the user, the file is transmitted electronically in units called packets. Each packet includes a header, and part of the information included in the header is the destination address where the information is being sent. See LANProtect at 5 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail me transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses.").

In addition, it would have been obvious to use the network file server/scanning system disclosed by LANProtect at a mail server, and implementing an FTP proxy server and an FTP daemon.

To the extent not already expressly or inherently present in LANProtect and TIS Firewall, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect, TIS Firewall and Hile to utilize an FTP proxy server and an FTP daemon as these were likely the most common file transfer proxy servers and daemons as of the Critical Date. Additionally, both Cheswick and Cheswick and Bellovin disclose the use of an FTP proxy server. Cheswick discloses use of an FTP proxy server in the context of providing incoming file transfers and Cheswick and Bellovin suggest use of an FTP server to facilitate secure file transfer through a firewall. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall and Hile are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

G. Whether claim 3 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick in view of Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper, and further in view of Hile

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the daemon is an SMTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the daemon is an SMTP daemon, raise a substantial new question of patentability with respect to claim 2 as pointed out in more detail below.

Claim 3 recites "the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

In total, Claim 3 adds as the specific proxy server type, "a SMTP proxy server". However, the restriction on the proxy server element to an SMTP proxy server is a meaningless restriction because the SMTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every electronic mail system as of the Critical Date.

Following is a high-level discussion of how Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 3.

Cheswick was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised. Cheswick discloses the use of SMTP proxy server that handles mail communication. See Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Datakit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked, and installed.")

Cheswick and Bellovin was not considered during prosecution of the ‘600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers. Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Sendmail program, and discusses the SMTP proxy in the context of security and filtering. *See* Cheswick and Bellovin at 189 (“A summary of the most common proxy connections [including SMTP] is shown in Table 11.1.”). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

LANProtect was not considered during the prosecution of the ‘600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect specifically notes scanning network traffic of any type. *See e.g.*, LANProtect at 5 (“All network traffic originating outside the file server (e.g., from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections.”). In addition, it would have been obvious to use the network file server/scanning system disclosed by LANProtect at a mail server, and implementing a SMTP proxy server and an SMTP daemon.

TIS Firewall was not considered during the prosecution of the ‘600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called “smap,” which stands for “Simple Mail Access Protocol.” See TIS Firewall at 8, (“SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TFS Manual was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network. TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See TFS Manual at 28. TFS Manual also mentions the message server software. See TFS Manual at 35 ("TFS requires both the Message Server software and API software to be active.")

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See MIMEsweeper at 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

Claim 3 adds the specific daemon type, an "SMTP daemon". However, the restriction on the daemon to an SMTP daemon is a hollow restriction as the SMTP daemon is, and was, a very common daemon, included on virtually every electronic mail system as of the Critical Date.

Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

Cheswick discloses the use of SMTP proxy server that handles mail communication. See Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Datakit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked, and installed.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Sendmail program, and discusses the SMTP proxy in the context of security and filtering. *See* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

In addition to the teachings regarding this claim element in Cheswick and Cheswick and Bellovin, LANProtect specifically notes scanning network traffic of any type. *See e.g.*, LANProtect at 5 ("All network traffic originating outside the file server (e.g., from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server/scanning system disclosed by LANProtect at a mail server, and implementing a SMTP proxy server and an SMTP daemon.

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin and LANProtect, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap," which stands for "Simple Mail Access Protocol." See TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall, TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See TFS Manual at 28. TFS Manual also mentions the message server software. See TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

In addition to the teachings regarding this claim element in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall and TFS Manual, MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See MIMEsweeper at 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

To the extent not already expressly or inherently present in LANProtect, TIS Firewall and MIMEsweeper, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect, TIS Firewall, MIMEsweeper and Hile to utilize an SMTP proxy server and an SMTP daemon as these were and remain very common processes that are included on virtually every electronic mail system. Additionally, both Cheswick and Cheswick and Bellovin disclose the use of an SMTP proxy server. Cheswick discloses use of an SMTP proxy to handle outgoing mail and Cheswick and Bellovin discusses the use of an SMTP proxy in the context of security and filtering. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, MIMEsweeper and Hile are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

I. Whether claim 4 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of TIS Firewall, and further in view of Sidewinder

None of Cheswick and Bellovin, TIS Firewall and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art considered during prosecution of the ‘600 patent taught or suggested “determining whether the data is of a type that is likely to contain a virus” and “transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.”

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 (“It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.”) And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 4 as pointed out in more detail below.

Claim 4 recites “A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:”

- receiving at a server a data transfer request including a destination address;
- electronically receiving data at the server;
- determining whether the data contains a virus at the server;
- performing a preset action on the data using the server if the data contains a virus;
- sending the data to the destination address if the data d determining whether the data is of a type that is likely to contain a virus; and does not contain a virus;
- determining whether the data is of a type that is likely to contain a virus; and
- transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.

(1) "receiving at a server a data transfer request including a destination address"

Cheswick and Bellovin was not considered during the prosecution of the '600 patent. It was published in 1994, to discuss a new paradigm in firewall and internet security. Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. In addition to the teachings regarding this claim element in Cheswick and Bellovin, TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

(2) "electronically receiving data at the server"

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

Cheswick and Bellovin describes that the incoming files are scanned for virus; therefore, the data is inherently received electronically at the location at which it is scanned. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

(3) "determining whether the data contains a virus at the server"

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Bellovin, TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs"). TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

(4) "performing a preset action on the data using the server if the data contains a virus"

Cheswick and Bellovin describe implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

TIS Firewall performs preset actions based on the content of the message, including the presence of a virus.

(5) "sending the data to the destination address if the data does not contain a virus"

Cheswick and Bellovin describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

In addition to the teachings regarding this claim element in Cheswick and Bellovin, TIS Firewall discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

Sidewinder was not considered during the prosecution of the '600 patent. Sidewinder teaches certain classes of data can be ***selectively*** prohibited from passing to and from the external network. In addition to the teachings regarding this claim element in Cheswick and Bellovin and TIS Firewall, Sidewinder discloses selectively sending data. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses").

(6) "determining whether the data is of a type that is likely to contain a virus"

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in Cheswick and Bellovin, Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses").

(7) "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus"

Sidewinder discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

None of Cheswick and Bellovin, TIS Firewall and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determining whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and taking a preset action if the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 4 as pointed out above.

To the extent not inherent or explicitly present in TIS Firewall and Cheswick and Bellovin, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify TIS Firewall and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by Sidewinder in order to avoid downstream virus infection. For example, Sidewinder teaches certain classes of data can be selectively prohibited from passing to and from the external network. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick and Bellovin, TIS Firewall and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115).

H. Whether claim 4 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall, and further in view of TFS Manual

None of LANProtect, TIS Firewall and TFS Manual were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art considered during prosecution of the '600 patent taught or suggested "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus."

Independent claim 4 relates to a computer-implemented method for detecting viruses at a server. It includes steps for checking for the presence of a virus in the data and transferring the data depending on the result of the virus check. Claim 4 also includes steps for determining whether the data is of a type that is likely to contain a virus and only determining whether a virus is present if the data is of a type that is likely to contain a virus. The steps of claim 4 are obvious in view of the above-listed combination of references as discussed below.

Claim 4: "A computer implemented method"

(1) "...for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:....."

Claim 4 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

TFS Manual was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network. TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses detecting viruses during file transfers between computers. *See, e.g.*, LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

(2) "…receiving at a server a data transfer request including a destination address;"

Claim 4 further recites "receiving at a server a data transfer request including a destination address."

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.*, TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages."); An incoming message directed to a recipient will have a destination address and this would be obvious to any person skilled in the art. The limitation of the data transfer request containing a destination address in inherent in the TFS Manual.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

(3) "…electronically receiving data at the server;..."

Claim 4 further recites "electronically receiving data at the server."

TFS Manual discloses a gateway wherein the mail message would necessarily be electronically received at the server.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is an inherent and fundamental aspect of any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

(4) "...determining whether the data contains a virus at the server;"

Claim 4 further recites "determining whether the data contains a virus at the server."

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

In addition to the teachings regarding this claim element in TFS Manual, LANProtect product literature expressly teaches this step. *See, e.g.*, LANProtect at pp. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses .... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

(5) "…performing a preset action on the data using the server if the data contains a virus;"

Claim 4 further recites "performing a preset action on the data using the server if the data contains a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

(6) "…sending the data to the destination address if the data does not contain a virus;"

Claim 4 further recites "sending the data to the destination address if the data does not contain a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

(7) "…determining whether the data is of a type that is likely to contain a virus; and;"

Claim 4 further recites "determining whether the data is of a type that is likely to contain a virus." As an initial matter, it is noted this is a common sense, efficiency mechanism, as it would not make sense to go to the effort of scanning data that is not likely to contain a virus.

TFS Manual discloses this claim element. The TFS Gateway described in TFS Manual would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. See TFS Manual at pg. 77 (example contents of a VIRUS.BAT file are shown in which only executable files are scanned). Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.*, LANProtect at p. 6 ("The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

(8) "…transmitting the data from the server to the destination without performing the steps of determining……"

Claim 4 further recites "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus."

TFS Manual discloses this claim element. If a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore, it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses that this step is performed by the LANProtect product. When the LANProtect product is configured to scan only those file types likely to contain a virus (e.g., DOS files with ".EXE" extension as configured by the user or administrator), LANProtect does not scan other file types or take any of the preset actions described above on the other file types, thereby meeting this limitation.

None of LANProtect, TIS Firewall and TFS Manual were considered during prosecution of the '600 patent. Each of these references contain a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 4 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify TIS Firewall to selectively transfer data based on the existence of viruses within such data as taught by TFS Manual and LANProtect in order to avoid downstream virus infection. For example, TFS Manual teaches different actions can be performed depending on the results of virus scanning (e.g., delete the file if a virus is detected vs. sending to its destination if no virus is detected). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in TIS Firewall, TFS Manual and LANProtect are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

J. Whether claim 5 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect

Claim 5 adds the limitation of storing the data in a temporary file to claim 4. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems as discussed below.

Claim 5: "storing the data in a temporary file at the server after the step of electronically transmitting;"

Claim 5 recites "The method of claim 4, further comprising the steps of storing the data in a temporary file at the server after the step of electronically transmitting; and wherein the step of determining includes scanning the data for a virus using the server."

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses the element of storage of the data in a temporary file at the server after the step of electronically transmitting and the step of determining by scanning the data for a virus using the server. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses…. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect was not considered during prosecution of the '600 patent. This prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and taking a preset action if the data contains a virus. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 4 as pointed out above.

To the extent not inherent or explicitly present in the combination of references applied to claim 4, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the combination of references to store data in a temporary file at the server after transmitting to support traditional logging functionality and allow a network administrator or the like to later review and evaluate same or to implement traditional quarantine functionality as taught by LANProtect. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in

LANProtect and the combination of references applied to claim 4 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

K. Whether claim 5 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall in view of Sidewinder, and further in view of MIMEsweeper

Claim 5 adds the limitation of storing the data in a temporary file to claim 4. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems. Claim 4 is rendered obvious by the combination of TIS Firewall with Sidewinder. The aspect of storing data in a temporary file at the server is disclosed by MIMEsweeper. See MIMEsweeper at 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

None of TIS Firewall, Sidewinder and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 5 as pointed out above.

To the extent not inherent or explicitly present in TIS Firewall with Sidewinder, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify TIS Firewall with Sidewinder to store data in a temporary file at the server after transmitting to support traditional logging functionality and allow a network administrator or the like to later review and evaluate same or to implement traditional quarantine functionality as taught by MIMEsweeper. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in TIS Firewall, MIMEsweeper and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

L. Whether claim 6 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall

Claim 6 adds a further limitation to claim 5 by claiming that the virus scanning is carried out by signature scanning process. The combination of the above-listed references as discussed below disclose the aspect of a signature scanning process.

Claim 6: "scanning is performed using a signature scanning process"

Claim 6 recites "The method of claim 5, wherein the step of scanning is performed using a signature scanning process." The oldest and most basic form of virus detection is signature scanning. Signature scanning typically involves a signature file (e.g., a database of uniquely identifiable "fingerprints" that a virus contains). The signature scanning process examines the machine code bytes—aka "strings" of the file at issue and determines whether one of the fingerprints is contained therein.

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses the element of signature scanning. The Intel Products performed a signature scanning process when scanning for viruses.

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. In addition to the teachings regarding this claim element in LANProtect, TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server and wherein the scanning is done via signature analysis. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 6 as pointed out above.

To the extent not inherent or explicitly present in the combination of references applied to claim 5, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the combination of references to perform signature scanning as taught by LANProtect and TIS Firewall as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, TIS Firewall and the combination of references applied to claim 5 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

M. Whether claim 6 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan

Claim 6 purports to add a further limitation to claim 5 by simply indicating the virus scanning is carried out by signature scanning process – the primary method of virus scanning at the time of filing of the '600 patent. Claim 6 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

MpScan was not considered during the prosecution of the '600 patent. MpScan discloses an e-mail content scanning firewall available prior to January 1994 that dealt with compressed data, dealt with uuencoded data and employed pattern matching to identify words, phrases or any other defined data in outgoing email. The aspect of signature scanning is suggested by MpScan, which renders obvious every limitation of claim 6 in combination with Cheswick and Bellovin and Sidewinder. See MpScan at 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new questions of patentability (SNQs) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 6 as pointed out above.

To the extent not inherent or explicitly present in Cheswick and Bellovin and Sidewinder, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheskwick and Bellovin and Sidewinder to perform signature scanning (pattern matching) as taught by MpScan as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheskwick and Bellovin, Sidewinder and MpScan are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

N. Whether claim 7 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TFS Manual

Dependent claim 7 further limits independent claim 4 by defining the preset steps that need to be taken to be one of a group including "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name". The preset steps of claim 7 are obvious in view of the references discussed below.

Claim 7: "preset action on the data using the server comprises performing one step from the group of"

Claim 7 recites "The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of: Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name"

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discusses aspects of new software that provides total LAN protection. LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

TFS Manual was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network. In addition to the teachings regarding this claim element in LANProtect, TFS Manual discloses a Gateway that would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

Neither LANProtect nor TFS Manual were considered during prosecution of the '600 patent. These references contain new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the preset step of "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 7 as pointed out above.

To the extent not inherent or explicitly disclosed in the references applied against claim 4, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to perform one of the present actions recited by claim 7 as taught by LANProtect and TFS Manual in order to avoid downstream virus infection (not transmitting the data), provide the data to the intended destination (transmit unchanged) or perform traditional quarantining functionality (store the data in a file with a new name and notify the recipient). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, TFS Manual and the references applied against claim 4 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

O. Whether claim 7 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of TIS Firewall

Claim 7 limits the types of actions that can represent the preset action of claim 4, reciting "The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of:"

- Transmitting the data unchanged;
- Not transmitting the data; and
- Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

Cheswick and Bellovin in combination with Sidewinder and TIS Firewall disclose every limitation of claim 4. The discussion of claim 4 is incorporated herein by reference. The further refinement of the "performing a preset action" step of claim 4 required by claim 7 is disclosed by

Sidewinder. Sidewinder discusses performing preset actions based on the content of the message, including the presence of a virus. In Sidewinder, messages which fail to pass the filter are passed to the System Administrator for action. Rejected mail may be discarded or kept in a 'trash' folder for later examination. Outgoing data which has been blocked by the filter is forwarded to the System Administrator for disposition. Incoming data which has been blocked by the filter is discarded (i.e., not transmitted). *See e.g.*, Sidewinder at SR-454.8 – SR-454.12 ("Messages which fail to pass the filter are forwarded to the System Administrator for action" and [the] System Administrator can block files or messages that don't pass the filter.)

In addition to the teachings regarding this claim element in Sidewinder, TIS Firewall performs preset actions based on the content of the message, including the presence of a virus.

None of Cheswick and Bellovin, Sidewinder and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 7 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Bellovin and TIS Firewall to perform one of the present actions recited by claim 7 as taught by Sidewinder in order to avoid downstream virus infection (not transmitting the data) or provide the data to the intended destination (transmit unchanged). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick and Bellovin, TIS Firewall and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115).

P. Whether claim 8 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TFS Manual

Dependent claim 8 further limits independent claim 4 by defining the determining step to include comparing an extension type of a file name for the data to a group or known extension types. The determining step of claim 8 is obvious in view of the combination of the above-listed references as discussed below.

Claim 8: "comparing an extension type of a file name for the data to a group or known extension types"

Claim 8 recites "The method of claim 4, wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group or known extension types."

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect discloses determining whether the data is of a type that is likely to contain a virus by comparing an extension type of a file name for the data to a group of known extension types. *See e.g.*, LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses…. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

TFS Manual was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network. In addition to the teachings regarding this claim element in LANProtect, TFS Manual discloses this claim element. The TFS Gateway described in TFS Manual would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

Neither LANProtect nor TFS Manual was considered during prosecution of the '600 patent. Both of these references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the determining step consisting of comparing extension type of a file name for the data to a group or known extension types. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 8 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the references applied to claim 4 to look at file extensions as taught by <u>LANProtect</u> and <u>TFS Manual</u> to allow configurability with respect to the types of files processed and/or to make virus scanning more efficient by avoiding scanning of those file types that are unlikely to contain a virus. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 4, <u>LANProtect</u> and <u>TFS Manual</u> are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

Q. Whether claim 8 is unpatentable under 35 U.S.C. § 103 as being obvious over <u>Cheswick and Bellovin</u> in view of <u>Sidewinder</u>, and further in view of <u>MIMEsweeper</u>

Dependent claim 8 further limits independent claim 4 by defining the determining step to include comparing an extension type of a file name for the data to a group or known extension types. Each element of claim 4 is disclosed by the combination of <u>Cheswick and Bellovin</u> and

Sidewinder. The discussion of Claim 4 is incorporated herein by reference. The limitation of claim 8 is further rendered obvious by Sidewinder and MIMEsweeper as discussed below.

Sidewinder determines whether the data is of a type that the program, user, or administrator believes is likely to contain a virus. *See e.g.*, Sidewinder at SR-454.9 - SR-454.10 ("The System Administrator also has the option to block all mail which does not fit the statistical properties of English-language plaintext. Such filtering effectively stops the use of the mail service as a means of sending or receiving dangerous, offensive, or illegal material such as virus-containing object code, personal encrypted messages, or pornographic pictures.").

MIMEsweeper determines whether the data is of a type that the program, user, or administrator believes is likely to contain a virus, see, e.g., MIMEsweeper at pg. 49 ("The way a file is scanned depends on the type of file … to be scanned and the validator employed.)

None of Cheswick and Bellovin, Sidewinder and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of comparing the extension type of the file name for the data to a group or known extension types. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 8 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Bellovin and Sidewinder to scan files depending on the type of file as taught by MIMEsweeper to allow configurability with respect to the types of files processed and manner of processing files. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheswick and Bellovin, Sidewinder, and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

R. Whether claim 9 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall

Dependent claim 9 restricts the steps of claim 4 to data transfers that are FTP transfers to the outbound transfers. The steps as recited by claim 9 are made obvious by TIS Firewall as discussed below:

Claim 9: "The method of claim 4, further comprising the steps of:"

(1) "...determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

Claim 9 recites "The method of claim 4, further comprising the steps of: determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate

the building of network firewalls. TIS Firewall determines whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.")

(2) "…wherein the server is a FTP proxy server;"

Claim 9 further recites "wherein the server is a FTP proxy server."

TIS Firewall discloses the use of an FTP server. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

(3) "…wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and;"

Claim 9 further recites "wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network."

TIS Firewall discloses this element. The step of electronically receiving data at the TIS Firewall includes the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination.").

(4) "…wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network;"

Claim 9 further recites "wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network."

TIS Firewall discloses this element. The step of electronically receiving data at the TIS Firewall comprised the steps of transferring the data from a server task to an FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination;" "As an example, the FTP proxy can block FTP export of files while permitting import of files, representing a granularity of control that router-based firewalls cannot presently achieve.").

TIS Firewall was not considered during prosecution of the '600 patent. TIS Firewall contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an outbound data transfer and steps of proceeding with the outbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

To the extent not inherent or explicitly disclosed by the references applied against claim 4, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to transfer data from a client node to the FTP proxy server as taught by <u>TIS Firewall</u> to facilitate outbound file transfers using a common file transfer mechanism. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 4 and <u>TIS Firewall</u> are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

S. Whether claim 9 is unpatentable under 35 U.S.C. § 103 as being obvious over <u>LANProtect</u> in view of <u>Sidewinder</u>

Dependent claim 9 restricts the steps of claim 4 to data transfers that are FTP transfers to the outbound transfers. The discussion regarding obviousness of claim 4 as discussed above is incorporated herein by reference. The steps recited by claim 9 are rendered obvious under 35 U.S.C. § 103(a) by <u>LANProtect</u> in view of <u>Sidewinder</u> as discussed below:

Claim 9 recites "The method of claim 4, further comprising the steps of:"

- determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;

- wherein the server is a FTP proxy server;
- wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and
- wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network

The combination of LANProtect and Sidewinder discloses each limitation of claim 4. Additionally, the combination of LANProtect and Sidewinder discloses each limitation of claim 9 as discussed below.

Sidewinder was capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

Sidewinder could be configured as an FTP proxy server. The step of electronically receiving data at the Sidewinder comprised the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network.

The step of electronically receiving data at the Sidewinder comprised the steps of transferring the data from a server task to an FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network.

Neither LANProtect nor Sidewinder were considered during prosecution of the ‘600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the ‘600 patent. As described herein, no prior art considered during prosecution of the ‘600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an outbound data transfer and steps of proceeding with the outbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect to transfer data from a client node to the FTP proxy server as taught by Sidewinder to facilitate outbound file transfers using a common file transfer mechanism. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

T. Whether claim 10 is unpatentable under 35 U.S.C. § 103 as being obvious over TIS Firewall

Dependent claim 10 restricts the steps of claim 4 to data transfers that are FTP transfers to the inbound transfers. The steps recited by claim 10 are obvious in view of TIS Firewall as discussed below.

Claim 10: "The method of claim 4, further comprising the steps of:"

(1) "...determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

Claim 10 recites "The method of claim 4, further comprising the steps of: determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. TIS Firewall determines whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.")

(2) "...wherein the server is a FTP proxy server;"

Claim 10 further recites "wherein the server is a FTP proxy server."

TIS Firewall discloses the use of an FTP server. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

(3) "...Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and"

Claim 10 further recites "Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network."

TIS Firewall discloses this element. The step of sending the data in the TIS Firewall comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination.").

(4) "…Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network."

Claim 10 further recites "wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network."

TIS Firewall discloses this element. The step of sending the data in the TIS Firewall comprised the steps of transferring the data from the FTP proxy server to an FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination;" "As an example, the FTP proxy can block FTP export of files while permitting import of files, representing a granularity of control that router-based firewalls cannot presently achieve.")

TIS Firewall was not considered during prosecution of the '600 patent. TIS Firewall contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an inbound data transfer and steps of proceeding with the inbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

To the extent not inherent or explicitly disclosed by the references applied against claim 4, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to transfer data from a client node to the FTP proxy server or from the FTP proxy server to a client node as taught by TIS Firewall to facilitate secure outbound and inbound file transfers using a common file transfer mechanism. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 4 and TIS Firewall are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

U. Whether claim 10 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of Sidewinder

Dependent claim 10 restricts the steps of claim 4 to data transfers that are FTP transfers to the inbound transfers. The discussion regarding obviousness of claim 4 as discussed above is incorporated herein by reference. The steps recited by claim 10 are rendered obvious under 35 U.S.C. § 103(a) by LANProtect in view of Sidewinder as discussed below:

Claim 10 recites "The method of claim 4, further comprising the steps of:"

- determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;
- wherein the server is a FTP proxy server;
- Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and
- Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

LANProtect discloses each limitation of claim 4. Additionally, Sidewinder discloses each limitation of claim 10 as discussed below.

Sidewinder was capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

Sidewinder could be configured as an FTP proxy server.

The step of sending data at the Sidewinder comprised transferring the data from the FTP proxy server to a client node, if the data is being transferred into the first network.

The step of sending the data at the Sidewinder comprised transferring the data from the FTP proxy server to an FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

Neither LANProtect nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an inbound data transfer and steps of proceeding with the inbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect to transfer data from a client node to the FTP proxy server or transfer data from the FTP proxy server to a client node as taught by Sidewinder to facilitate secure outbound and inbound file transfers using a common file transfer mechanism.

Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

V. Whether claim 11 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Neither LANProtect nor MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus was considered during prosecution of the '600 patent.

The teaching related to detecting the presence of a virus in an encoded portion of a mail message as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 11 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 11 of the '600 patent.

Claim 11: "A computer implemented method"

(1) "...for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"

Claim 11 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.*, LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.*, LANProtect at pg. 16 ("Direction of I/O to scan-LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses. In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

(2) "…receiving a mail message request including a destination address;"

Claim 11 further recites "receiving at a server a data transfer request including a destination address."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server involved receiving requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

(3) "…electronically receiving data at the server;"

Claim 11 further recites "electronically receiving data at the server."

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper electronically receives mail messages at the server. *See e.g.,* MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art. MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

(4) "…determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;"

Claim 11 further recites "whether the mail message contains a virus…"

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches a scanning process that is preconfigured and that can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores.

See e.g., MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the

Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper's container handling architecture allows decompression of Email message attachment contents."). Since, the Minesweeper extracts all the elements of the email message before presenting them to external programs called "Validators" for virus scanning, the storing of these extracted elements in separate temporary files would be obvious to any person skilled in the art.

(5) "…performing a preset action on the mail message if the mail message contains a virus; and"

Claim 11 further recites "performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(6) "…sending the mail message to the destination address if the mail message does not contain a virus."

Claim 11 further recites "sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches allowing transfer of the data to the destination address. The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine LANProtect and MIMEsweeper so as to selectively transfer data based on the existence of viruses in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to identify, decode and scan encoded portions of a mail message as taught by LANProtect and MIMEsweeper as most email attachments as of the Critical Date and to this day use the MIME (Multipurpose Internet Mail Extensions) format. In this manner, the virus scanning engine would be able to parse MIME files to find the target files and then scan them as desired. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

W. Whether claim 11 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper and Sidewinder, and further in view of MpScan

None of LANProtect, MIMEsweeper, MpScan and Sidewinder were considered during prosecution of the ‘600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the ‘600 patent. As shown above, no prior art concerning the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus was considered during prosecution of the ‘600 patent.

As such, the substantial new questions of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 (“It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the scanning of the mail messages for the presence encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus raise a substantial new question of patentability with respect to claim 11 as pointed out in more detail below.

Claim 11 recites "A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer", the method comprising the steps of:

- receiving a mail message request including a destination address;
- electronically receiving the mail message at a server;
- determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses;
- performing a preset action on the mail message if the mail message contains a virus; and
- sending the mail message to the destination address if the mail message does not contains a virus.

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.*, LANProtect at pg. 2 (“LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity.”). *See e.g.*, LANProtect at 16 (“Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.”).

LANProtect discloses receiving a data transfer request including a destination address. As LANProtect runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the data file.

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 (“Scan both incoming and outgoing files on the server with the Real Time scan”). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User’s Guide at pg. ii (“Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded”).

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 (“All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.”).

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

However if the aspect of "the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;" was somehow construed so that LANProtect did not practice this aspect, this element is disclosed or suggested by MpScan and Sidewinder as discussed below.

MpScan was not considered during the prosecution of the '600 patent. MpScan discloses an e-mail content scanning firewall available prior to January 1994. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder was not considered during the prosecution of the '600 patent. Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in September of 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses. MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server received requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper electronically receives mail messages at the server. *See e.g.,* B MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scanning process is preconfigured and can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper's container handling architecture allows decompression of Email message attachment contents."). Since, the Minesweeper extracts all the elements of the email message before presenting them to external programs called “Validators” for virus scanning, the storing of these extracted elements in separate temporary files would be obvious to any person skilled in the art.

MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called ‘Validators’. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

Further, if a file does not contain a virus, the MIMEsweeper allows transfer of the data to the destination address. The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 (“Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.”).

However if the aspect of “the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;” was somehow construed so that MIMEsweeper did not practice this aspect, this element is disclosed or suggested by MpScan and Sidewinder as discussed below.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.*, Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

None of LANProtect, MIMEsweeper, MpScan and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus. As such, the substantial new question of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 11 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine LANProtect, MIMEsweeper, Sidewinder and MpScan so as to selectively transfer data based on the existence of viruses in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to modify Sidewinder and MpScan to identify, decode and scan encoded portions of a mail message as taught by LANProtect and MIMEsweeper as most email attachments as of the Critical Date and to this day use the MIME (Multipurpose Internet Mail Extensions) format. In this manner, the virus scanning engine would be able to parse MIME files to find the target files and then scan them as desired. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper, Sidewinder and MpScan are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

X. Whether claim 12 is unpatentable under 35 U.S.C. § 103 as being obvious over MpScan in view of MIMEsweeper

Claim 12 further refines the step of "determiing whether the mail message includes any encoded portions" of claim 11 to require searching for uuencoded portions. UUencoding was a well-known and common mechanism for encoding binary data for transmission as of the filing date of the '600 patent. As such, this purported further refinement of claim 12 does not serve to patentably distinguish the claim and this claim is obvious for at least the same reasons as pointed out with reference to claim 11.

In addition, the combination of MpScan and MIMEsweeper as discussed below render obvious this limitation. The teaching related to the scanning of the mail messages for the presence of "uuencoded" portions as contained in the above-listed references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 12 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 12 of the '600 patent.

> **Claim12: "The method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions."**

Claim 12 recites "the method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions."

MpScan was not considered during the prosecution of the '600 patent. MpScan discloses an e-mail content scanning firewall available prior to January 1994. MpScan describes the aspect of receiving a mail message request including a destination address. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses. In addition to the teachings regarding this claim element in MpScan, MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.").

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine MIMEsweeper and MpScan so as to identify and scan uuencoded portions in order to remain backward compatible with legacy systems that use uuencode for encoding binary data for transmission and to allow such uuencoded portions to be effectively scanned for viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in MpScan and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

Y. Whether claim 13 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Neither LANProtect nor MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of a proxy server and a daemon in connection with removing a virus in data transfers was considered during prosecution of the '600 patent, which elements were mistakenly considered points of novelty by the Examiner in allowing such claims.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

Claim 13: "A computer implemented method"

(1) "…for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"

Claim 13 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity.”). *See e.g.,* LANProtect at pg. 16 (“Direction of I/O to scan-LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.”).

MIMEsweeper was not considered during the prosecution of the ‘600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses. In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 (“MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.”).

(2) “…receiving a mail message request including a destination address;”

Claim 13 further recites “receiving at a server a mail message request including a destination address.”

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches receiving a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server involved receiving requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.*, MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

(3) "...electronically receiving the mail message at the server;"

Claim 13 further recites "electronically receiving the mail message at the server."

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches electronically receiving mail messages at the server. *See e.g.*, MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

(4) "…scanning the mail message for encoded portions; determining whether the mail message contains a virus;"

Claim 13 further recites "whether the mail message contains a virus…"

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches a scanning process that is preconfigured and that can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.").

(5) "…performing a preset action on the mail message if the mail message contains a virus;"

Claim 13 further recites "performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(6) "…sending the mail message to the destination address if the mail message does not contain a virus; and"

Claim 13 further recites "sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper allows transfer of the data to the destination address. MIMEsweeper teaches examining the messages and based upon the results of the analysis, submitting the message for onward transmission, or diverting it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

(7) "…wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address."

Claim 13 further recites "sending the data to the destination address if the data does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message to its destination involves transferring of mail message from the SMTP proxy server to the SMTP daemon and thereafter transferring the message from SMTP daemon to its final destination."

LANProtect specifically discloses the scanning of the network traffic of any type. *See e.g.,* LANProtect at pg. 6 ("All network traffic originating outside the file server (e.g. from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server system/scanning system disclosed by LANProtect at the mail server and in addition implementing a SMTP proxy server and an SMTP daemon.

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* MIMEsweeper at pg. 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine LANProtect and MIMEsweeper so as to selectively transfer data based on the existence of viruses in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

Z. Whether claim 13 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin and TIS Firewall, and further in view of TFS Manual

None of LANProtect, MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination address was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination raise a substantial new question of patentability with respect to claim 13 as pointed out in more detail below.

Claim 13: "A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"

- receiving a mail message request including a destination address;
- electronically receiving the mail message at the server;
- scanning the mail message for encoded portions; determining whether the mail message contains a virus;
- performing a preset action on the mail message if the mail message contains a virus;
- sending the mail message to the destination address if the mail message does not contain a virus; and
- wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address."

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan-LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

LANProtect specifically discloses the scanning of the network traffic of any type. *See e.g.,* LANProtect at pg. 6 ("All network traffic originating outside the file server (e.g. from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server system/scanning system disclosed by LANProtect at the mail server and in addition implementing a SMTP proxy server and an SMTP daemon.

However if the aspect of "scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination" was somehow construed so that LANProtect did not practice this aspect, this element is disclosed or suggested by a set of prior art including MpScan, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

Cheswick discloses the use of SMTP proxy server that handles the mail communication. *See e.g.,* Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Data kit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also discloses the use of a server daemon in a gateway system. *See e.g.,* Cheswick at 234 ("Our new gateway machine named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.")

In addition, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Send-mail program, and discusses the SMTP proxy in the context of security and filtering. *See e.g.,* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

Additionally, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition, the TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* TFS Manual at 28. TFS Manual also discloses the message server software. *See e.g.,* TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses. MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination.

Since the SMTP server involved receiving requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper electronically receives mail messages at the server. *See e.g.,* MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scanning process is preconfigured and can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further.”). *See e.g.,* MIMEsweeper at pg. 9 (“The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded.”). *See e.g.,* MIMEsweeper at pg. 9 (“MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.”).

MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called ‘Validators’. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

Further, if a file does not contain a virus, MIMEsweeper allows transfer of the data to the destination address. MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 (“Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.”).

MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* MIMEsweeper at pg. 13 (“The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

However if the aspect of "scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination" was somehow construed so that MIMEsweeper did not practice this aspect, this element is disclosed or suggested by a set of prior art including MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.*, MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.*, Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

Cheswick discloses the use of SMTP proxy server that handles the mail communication. *See e.g.,* Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Data kit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. *See e.g.,* Cheswick at 234 ("Our new gateway machine named inet, is a MIPS M/120 running System V with

Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.")

In addition, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Send-mail program, and discusses the SMTP proxy in the context of security and filtering. *See e.g.,* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

Additionally, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition, TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* TFS Manual at 28. TFS Manual also discloses the message server software. *See e.g.,* TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

None of LANProtect, MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent.

As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the received mail messages for the presence of encoded portions at the sever and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 13 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheswick and Cheswick and Bellovin to selectively transfer data based on the existence of viruses within such data as taught by LANProtect, TIS Firewall, Sidewinder, TFS Manual and MIMEsweeper in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to utilize proxy servers as intermediaries to forward IP traffic and daemons to perform background processing as firewalls and gateways during that time frame routinely and customarily implemented proxy servers and daemons in the context of providing scanning and security services as evidenced by Cheswick and Cheswick and Bellovin. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and TIS Firewall cites to Cheswick (see, e.g., TIS Firewall at pg. 14).

AA. Whether claim 14 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Claim 14 simply adds unremarkable limitations relating to storing the message in a temporary file and scanning the temporary file to determine whether the message contains a virus to claim 11. As this is an obvious implementation detail that does not patentably distinguish the claim over the references applied to claim 11, claim 14 is obvious for at least the reasons presented above with reference to claim 11.

In addition, the combination of LANProtect and MIMEsweeper as discussed below render obvious this limitation.

Claim14: "The method of claim 11,"

(1) "…wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"

Claim 14 recites "the method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

MIMEsweeper was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses. In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

(2) "…storing the message in a temporary file;"

Claim 14 further recites "storing the message in a temporary file."

LANProtect discloses the element of storage of data in a temporary file at the server and thereafter scanning the file for the presence of the viruses. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files specified as 'all' or by specific file extension).").

In addition to the teachings regarding this claim element in LANProtect, The aspect of storing data in a temporary file at the server is disclosed by MIMEsweeper. *See e.g.,* MIMEsweeper at pg. 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

(3) "…scanning the temporary file for viruses; and testing whether the scanning step found a virus.'

Claim 14 further recites "scanning the temporary file for viruses and testing whether the scanning step found a virus."

LANProtect discloses the element of storage of data in a temporary file at the server and thereafter scanning the data for a virus using the server. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches checking the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

As indicated above, neither LANProtect nor MIMEsweeper were considered during prosecution of the '600 patent and these references contain new, non-cumulative technological teachings specifically not present during the prosecution of the '600 patent. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect to store messages in temporary files for scanning as taught by MIMEsweeper in order have the messages in a form and location suitable for analysis. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

BB. Whether claim 14 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, TIS Firewall, Sidewinder, MpScan and Layland, and further in view of Hile

None of MIMEsweeper, TIS Firewall, Sidewinder, MpScan, Layland were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the storing of the messages in temporary files and thereafter scanning the messages for the presence of the viruses was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the storage of the messages in the temporary files and thereafter scanning the temporary files for the presence of the viruses raise a substantial new question of patentability with respect to claim 14 as pointed out in more detail below.

Claim 14 recites "The method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:

- storing the message in a temporary file;
- scanning the temporary file for viruses; and
- testing whether the scanning step found a virus."

Claim 14 adds the limitation of storing the data in a temporary file to claim 11. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems. Claim 14 is rendered obvious in view of the combination of LANProtect, MIMEsweeper, TIS Firewall, Sidewinder, MpScan, Layland and Hile.

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan-LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

LANProtect discloses the element of storage of the data in a temporary file at the server and thereafter scanning the file for the presence of the viruses. See e.g., LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files specified as 'all' or by specific file extension).").

LANProtect discloses the element of storage of the data in a temporary file at the server and thereafter scanning the data for a virus using the server. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

However if the aspect of "storing the messages in temporary files and thereafter scanning the temporary files for the presence of the viruses" was somehow construed so that LANProtect did not practice this aspect, this element is disclosed or suggested by a set of prior art including TIS Firewall, Sidewinder, MpScan, Layland as discussed below.

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. In TIS Firewall, the encoded portion is stored in separate temporary storage. The "?" character is decoded by replacement with a "#" character and the following address site is scanned for other "?" characters. Based on the test of whether any other "?" characters are found, further replacements are made. *See e.g.,* TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems"), TIS Firewall at pg. 10 ("if there is a security hole in fingerd, it cannot be effectively exploited, since no file system or executables will be available to the attacker").

Sidewinder was not considered during the prosecution of the '600 patent. Sidewinder teaches certain classes of data can be ***selectively*** prohibited from passing to and from the external network. Sidewinder teaches routines that can store mail messages in storage based on content or presence of object code containing viruses and then scan those messages for viruses. *See e.g.,* Sidewinder at SR-454.1 – SR-454.2 ("Sidewinder is an application-level secure gateway between TCP/IP networks and incorporates the patented Type Enforcement mechanism"), 2858 (discusses Type Enforcement and data filtering), SR-454.9 – SR-454.11 (the Sidewinder System Administrator can filter mail based on destination or content).

MpScan was not considered during the prosecution of the '600 patent. MpScan discloses an e-mail content scanning firewall available prior to January 1994. MpScan describes the aspect of receiving a mail message and performing the pattern matching of the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. To the extent the reference doesn't explicitly disclose whether the mail messages are stored in temporary files or in some other form of storage, in order to perform the pattern matching of outgoing email, it would have been obvious to use a temporary file to store messages temporarily. *See e.g.,* MpScan pg. 1-2.

Layland was not considered during prosecution of the '600 patent. Layland suggests use of an Internet gateway that subjects all incoming files to a virus scan by storing mail messages, for example, in temporary files or in some other form of storage prior to the scanning of the data for the presence of the viruses. *See e.g.,* Layland at pg. 23-24 ("The router would send all traffic to and from the Internet to the gateway for approval and processing before routing the traffic to its destination.... The Internet Gateway would subject all incoming files to a virus scan.") In order to scan the incoming files, it would have been obvious to use the temporary files or some other means of storage for storing or buffering the incoming files.

The teachings as contained in TIS Firewall, Sidewinder, MpScan and Layland were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. Hile teaches storing of data in a temporary file, scanning the temporary file for virus, and determining if a virus is present or not. *See e.g.,* col. 4, ll. 7-26.

As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 14 is patentable. For this reason, the teachings of Hile in combination with the teachings of TIS Firewall, Sidewinder, MpScan and Layland raise a substantial new question of patentability with respect to at least claim 14 of the '600 patent.

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. The MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses. MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments."). The aspect of storing the data in a temporary file at the server is disclosed by MIMEsweeper. *See e.g.,* MIMEsweeper at pg. 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 (“The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.”).

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 (“MIMEsweeper as mail transfer agent”). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

However if the aspect of “storing the messages in temporary files and thereafter scanning the temporary files for the presence of the viruses” was somehow construed so that MIMEsweeper did not practice this aspect, this element is disclosed or suggested by a set of prior art including TIS Firewall, Sidewinder, MpScan and Layland as discussed below.

In the TIS Firewall, the encoded portion is stored in separate temporary storage. The “?” character is decoded by replacement with a “#” character and the following address site is scanned for other “?” characters. Based on the test of whether any other “?” characters are found, further replacements are made. *See e.g.,* TIS Firewall at pg. 10, FN 3 (“The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems”), TIS Firewall at pg. 10 (“if there is a security hole in fingerd, it cannot be effectively exploited, since no file system or executables will be available to the attacker").

In addition, Sidewinder teaches routines that can store mail messages in storage based on content or presence of object code containing viruses and then scan those messages for viruses. *See e.g.,* Sidewinder at SR-454.1 – SR-454.2 ("Sidewinder is an application-level secure gateway between TCP/IP networks and incorporates the patented Type Enforcement mechanism"), 2858 (discusses Type Enforcement and data filtering), SR-454.9 – SR-454.11 (the Sidewinder System Administrator can filter mail based on destination or content).

Furthermore, MpScan describes the aspect of receiving a mail message and performing the pattern matching of the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. To the extent the reference doesn't explicitly disclose whether the mail messages are stored in temporary files or in some other form of storage, in order to perform the pattern matching of outgoing email, it would have been obvious to use a temporary file to store messages temporarily. *See e.g.,* MpScan pg. 1-2.

Layland indicates the storage of mail messages in temporary files or in some other form of storage prior to the scanning of the data for the presence of the viruses. *See e.g.,* Layland at pg. 23-24 ("The router would send all traffic to and from the Internet to the gateway for approval and processing before routing the traffic to its destination.... The Internet Gateway would subject all incoming files to a virus scan.") In order to scan the incoming files, it would have been obvious to use the temporary files or some other means of storage for storing or buffering the incoming files.

The teachings as contained in TIS Firewall, Sidewinder, MpScan and Layland were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. Hile teaches storing of data in a temporary file, scanning the temporary file for viruses, and determining if a virus is present or not. *See e.g.,* col. 4, ll. 7-26.

As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 14 is patentable. For this reason, the teachings of Hile in combination with the teachings by MIMEsweeper, TIS Firewall, Sidewinder, MpScan and Layland raise a substantial new question of patentability with respect to at least claim 14 of the '600 patent.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify LANProtect and Hile to store messages in temporary files for scanning as taught by MIMEsweeper, TIS Firewall, Sidewinder, MpScan and Layland in order have the messages in a form and location suitable for analysis. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper, TIS Firewall, Sidewinder, MpScan, Layland and Hile are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

CC. Whether claim 15 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall

Claim 15 adds a further limitation to claim 11 by claiming that the virus scanning is carried out by signature scanning process. LANProtect and TIS Firewall disclose the aspect of signature scanning process of virus detection. As noted above, the oldest and most basic form of virus detection is signature scanning. Signature scanning typically involves a signature file (e.g., a database of uniquely identifiable "fingerprints" that a virus contains). The signature scanning process examines the machine code bytes—aka "strings" of the file at issue and determines whether one of the fingerprints is contained therein.

Claim 15: "scanning is performed using a signature scanning process"

Claim 15 recites "The method of claim 11, wherein the step of scanning is performed using a signature scanning process."

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses the element of signature scanning. The Intel Products performed the signature scanning process while scanning for viruses. See, e.g., LANProtect at pg. 4-10.

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls. In addition to the teachings regarding this claim element in LANProtect, TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus wherein the scanning for virus is done via signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 15 as pointed out above.

To the extent not inherent or explicitly present in the combination of references applied to claim 11, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the combination of references to perform signature scanning as taught by LANProtect and TIS Firewall as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, TIS Firewall and the combination of references applied to claim 11 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

DD. Whether claim 15 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan

Claim 15 adds a further limitation to claim 11 by claiming that the virus scanning is carried out by signature scanning process. Claim 15 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

The aspect signature scanning is suggested by MpScan and renders every limitation of claim 15 obvious in combination with Cheswick and Bellovin and Sidewinder. See MpScan at 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus wherein the scanning for virus is done via signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 15 as pointed out above.

To the extent not inherent or explicitly present in Cheswick and Bellovin and Sidewinder, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheskwick and Bellovin and Sidewinder to perform signature scanning (pattern matching) as taught by MpScan as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheskwick and Bellovin, Sidewinder and MpScan are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

EE. Whether claim 16 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Dependent claim 16 purports to refine the step of "performing a preset action on the mail message" of claim 11 to (i) transferring the mail message unchanged, (ii) not transferring the mail message, (iii) storing the mail message as a file with a new name and notifying the recipient, or (iv) creating a modified mail message.

Neither LANProtect nor MIMEsweeper were considered during prosecution of the '600 patent. These references contain, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the preset step of "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability.

Claim16: "The method of claim 11, wherein

(1) …the step of performing a preset action on the mail message comprises performing one step from the group of:"

Claim 16 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(2) "…transferring the mail message unchanged;"

Claim 16 further recites "transferring the mail message unchanged."

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

(3) "…not transferring the mail message;"

Claim 16 further recites "not transferring the mail message."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the aspect of not transferring the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(4) "…storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and"

Claim 16 further recites "storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found.”). See also LANProtect at pg. 2-4 (“The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.”).

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called ‘Validators’. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(5) “…creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.”

Claim 16 further recites “creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.”

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and further archiving log files to the removable media which contain the output of the determining step. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

To the extent not inherent or explicitly disclosed in the references applied against claim 11, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to perform one of the present actions recited by claim 16 as taught by

LANProtect and MIMEsweeper in order to avoid downstream virus infection (not transmitting the data), provide the data to the intended destination (transmit unchanged) or perform traditional quarantining functionality (store the data in a file with a new name and notify the recipient). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper and the references applied against claim 11 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

FF. Whether claim 16 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address raise a substantial new question of patentability with respect to claim 16 as pointed out in more detail below.

Claim 16 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

- transferring the mail message unchanged;
- not transferring the mail message;
- storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and
- creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection. LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address;" was somehow construed so that LANProtect did not practice this aspect, this element is disclosed or suggested by a set of prior art including Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below.

Sidewinder was not considered during the prosecution of the '600 patent. Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

TIS Firewall was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate

the building of network firewalls. In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. It suggests the Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

SunScreen SPF-100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF 100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF 100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded. SunScreen SPF-100 discloses some of the aspects of claim 16. The SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses. MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address;" was somehow construed so that MIMEsweeper did not practice this aspect, this element is disclosed or suggested by a set of prior art including Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 16. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 16 as pointed out above.

To the extent not inherent or explicitly disclosed in TIS Firewall, Layland and SunScreen SPF-100, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to perform one of the present actions recited by claim 16 as taught by LANProtect, TFS Manual and MIMEsweeper in order to avoid downstream virus infection (not transmitting the data), provide the data to the intended destination (transmit unchanged) or perform traditional quarantining functionality (store the data in a file with a new name and notify the recipient). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in TIS Firewall, Layland, SunScreen SPF-100, LANProtect, TFS Manual and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

GG. Whether claim 17 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Dependent claim 17 purports to refine the step of "performing a preset action on the mail message" of claim 11 in a manner similar to dependent claim 16. As such, dependent claim 17 is obvious for at least the reasons noted above with reference to dependent claim 16.

The teaching related to the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 17 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 17 of the '600 patent.

Claim17: "The method of claim 11, wherein

(1) …the step of performing a preset action on the mail message comprises performing one step from the group of:"

Claim 17 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(2) "...transferring the mail message unchanged;"

Claim 17 further recites "transferring the mail message unchanged."

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg.

10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

(3) "…transferring the mail message with the encoded portions having a virus deleted;"

Claim 17 further recites "transferring the mail message with the encoded portions having a virus deleted."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

(4) "…renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and"

Claim 17 further recites “renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory.”

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 (“This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found.”). See also LANProtect at pg. 2-4 (“The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.”).

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called ‘Validators’. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(5) "….writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."

Claim 17 further recites "writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and further archiving log files to the removable media which contain the output of the determining step. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine LANProtect and MIMEsweeper so as to transfer the mail message with the encoded portions having a virus deleted in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to identify, decode and scan encoded portions of a mail message as taught by LANProtect and MIMEsweeper as most email attachments as of the Critical Date and to this day use the MIME (Multipurpose Internet Mail Extensions) format. In this manner, the virus scanning engine would be able to parse MIME files to find the target files, scan them and then treat them as desired. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and MIMEsweeper are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

HH. Whether claim 17 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message raise a substantial new question of patentability with respect to claim 17 as pointed out in more detail below.

Claim 17 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

- transferring the mail message unchanged;
- transferring the mail message with the encoded portions having a virus deleted; and
- renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and
- writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message;" was somehow construed so that LANProtect did not practice this aspect, this element is disclosed or suggested by a set of prior art including Sidewinder, the TIS Firewall, Layland and SunScreen SPF-100 as discussed below.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

SunScreen SPF 100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded. SunScreen SPF-100 discloses some of the aspects of claim 17. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action on the mail message comprising of either of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message." was somehow construed so that MIMEsweeper did not practice this aspect, this element is disclosed or suggested by a set of prior art including Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 17. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 17 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to combine LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 so as to transfer the mail message with the encoded portions having a virus deleted in order to avoid downstream virus infection. It would have also been obvious to one or ordinary skill in the art at the time the alleged invention was made to identify, decode and scan encoded portions of a mail message as taught by LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as most email attachments as of the Critical Date and to this day use the MIME (Multipurpose Internet Mail Extensions) format. In this manner, the virus scanning engine would be able to parse MIME files to find the target files, scan them and then treat them as desired. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

II. Whether claim 18 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect and Cheswick and Bellovin and TIS Firewall, and further in view of Hile

None of TFS Manual, LANProtect, Cheswick and Bellovin and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, while Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 18 as pointed out in more detail below.

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:

- means for receiving a data transfer request including a destination address;
- means for electronically receiving data at a server; means for determining whether the data contains a virus at the server;
- means for performing a preset action on the data using the server if the data contains a virus; and
- means for sending the data to the destination address if the data does not contain a virus.

Following is a high-level discussion of how the TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 18. A more detailed element-by-element analysis is presented below.

TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

The TFS Manual discloses a gateway wherein the mail message would be electronically received at the server.

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. *See e.g.,* TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

TFS Gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

Furthermore, LANProtect can detect viruses during file transfers between computers. *See, e.g.* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address and data being received electronically adds a meaningless limitation to claim 18. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

LANProtect product literature confirms that LANProtect performed this step. *See, e.g.* LANProtect at pg. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses …. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall

Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

Cheswick and Bellovin describes that the incoming files are scanned for virus therefore the data is received electronically. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

In addition, the TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9(smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

TIS Firewall performs preset actions based on the content of the message, including the presence of a virus. The TIS Firewall replaces the "|" character with a "#" character (modify), writes the file to a holding area (sequester) and logs the event (alert), only if the address portion of the mail message contains a "|" character.

TIS Firewall discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

The teachings as contained in TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 18 is patentable. For this reason, the teachings of Hile in combination with the teachings by TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall raise a substantial new question of patentability with respect to at least claim 18 of the '600 patent.

Independent claim 18 relates to an apparatus for detecting viruses in the data transfers between two computers at a server. It includes steps for checking for the presence of a virus in the data and transferring the data depending on the result of the virus check. Claim 18 also includes steps for performing preset action on the data if the data contains virus. The steps of claim 18 are obvious in view of the above-listed combination of references as described in further detail below.

Claim 18: "An apparatus"

(1) "...for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

In addition to the teachings regarding this claim element in TFS Manual, LANProtect can detect viruses during file transfers between computers. *See, e.g.* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. *See e.g.,* Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. *See e.g.,* Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. *See e.g.,* Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

(2) "…means for receiving a data transfer request including a destination address;"

Claim 18 further recites "means for receiving a data transfer request including a destination address."

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

In addition to the teachings regarding this claim element in TFS Manual, LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. *See e.g.,* Cheswick and Bellovin at pg. 66-69 and 74-75.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

(3) "…means for electronically receiving data at a server;"

Claim 18 further recites "means for electronically receiving data at a server."

The TFS Manual discloses a gateway wherein the mail message would be electronically received at the server.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address and data being received electronically adds a meaningless limitation to claim 18. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin describes that the incoming files are scanned for virus therefore the data is received electronically. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

(4) "…means for determining whether the data contains a virus at the server;"

Claim 18 further recites "means for determining whether the data contains a virus at the server."

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. *See e.g.,* TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

In addition to the teachings regarding this claim element in TFS Manual, LANProtect product literature confirms that LANProtect performed this step. *See, e.g.* LANProtect at pg. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses …. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

(5) "…means for performing a preset action on the data using the server if the data contains a virus; and"

Claim 18 further recites "means for performing a preset action on the data using the server if the data contains a virus."

TFS Gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall teaches performing preset actions based on the content of the message, including the presence of a virus.

(6) "…means for sending the data to the destination address if the data does not contain a virus."

Claim 18 further recites "means for sending the data to the destination address if the data does not contain a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. *See e.g.*, TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

In addition to the teachings regarding this claim element in TFS Manual and LANProtect, Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

In addition to the teachings regarding this claim element in TFS Manual, LANProtect and Cheswick and Bellovin, TIS Firewall discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

To the extent not inherent or explicitly taught by Cheswick and Bellovin, TIS Firewall and Hile, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to selectively transfer data based on the existence of viruses within such data as taught by TFS Manual and LANProtect in order to avoid downstream virus infection. For example, TFS Manual teaches different actions can be performed depending on the results of virus scanning (e.g., delete the file if a virus is detected vs. sending to its destination if no virus is detected). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall and Hile are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection. Finally, a further motivation to combine the teachings of Cheswick and Bellovin with those of TIS Firewall is the fact that Cheswick and Bellovin expressly includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115).

JJ. Whether claim 19 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of TIS Firewall

Claim 19 adds a further limitation to claim 18 by claiming that the virus scanning is carried out by signature scanning process. The combination of the above-listed references as discussed below disclose the aspect of signature scanning.

Claim 19: "scanning is performed using a signature scanning process"

Claim 19 recites "The apparatus of claim 18, wherein means for determining includes a means for scanning that scans the data using a signature scanning process."

LANProtect discloses the element of signature scanning. The Intel Products performed the signature scanning process while scanning for viruses. See, e.g., LANProtect at pg. 4-10.

In addition to the teachings regarding this claim element in LANProtect, TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning. *See e.g.,* TIS Firewall at pg. 41 (since many attacks "have a distinctive signature smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the ‘600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the ‘600 patent. As described herein, no prior art considered during prosecution of the ‘600 patent concerns the aspect of scanning the data for the presence of the viruses at the server wherein the scanning for virus is done via signature analysis. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 (“It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.”) And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 19 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the combination of references to perform signature scanning as taught by LANProtect and TIS Firewall as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect and TIS Firewall are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

KK. Whether claim 19 is unpatentable under 35 U.S.C. § 103 as being obvious over Cheswick and Bellovin in view of Sidewinder, and further in view of MpScan

Claim 19 adds a further limitation to claim 18 by claiming that the virus scanning is carried out by signature scanning process. Claim 19 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

The aspect signature scanning is suggested by MpScan and renders every limitation of claim 19 obvious in combination with Cheswick and Bellovin and Sidewinder. *See e.g.,* MpScan pg. 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the data for the presence of the viruses wherein the scanning for virus is done via signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 19 as pointed out above.

To the extent not inherent or explicitly present in Cheswick and Bellovin and Sidewinder, it would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify Cheskwick and Bellovin and Sidewinder to perform signature scanning (pattern matching) as taught by MpScan as this would facilitate the identification of known or configured viruses in the data. Furthermore, signature scanning is a very common and easily implemented method of identifying the existence of viruses. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in Cheskwick and Bellovin, Sidewinder and MpScan are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

LL. Whether claim 20 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect in view of MIMEsweeper

Dependent claim 20 purports to refine the means of "performing a preset action on the mail message" of claim 18 to (i) a means for transferring the mail message unchanged, (ii) a means for not transferring the mail message, or (iii) a means for storing the mail message as a file with a new name and notifying the recipient. As such, dependent claim 20 is obvious for at least the reasons noted above with reference to dependent claim 16.

The teaching related to the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 20 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 20 of the ‘600 patent.

Claim20: “The apparatus of claim 18, wherein

(1) … the means for performing a preset action comprises:”

Claim 20 recites “The apparatus of claim 18, wherein the means for performing a preset action comprises:”

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 (“LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.”). *See e.g.*, LANProtect at pg. 15 (“Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.”). See e.g., LANProtect at pg. 11 (“When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.”).

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 (“MIMEsweeper as mail transfer agent”). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

(2) "…means for transmitting the data unchanged;"

Claim 20 further recites "means for transmitting the data unchanged;"

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the transfer of the data/ mail messages unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg.

10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

(3) "…means for not transmitting the data"

Claim 20 further recites "means for not transmitting the data"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the aspect of not transferring the infected mail message/ data depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(4) "…means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."

Claim 20 further recites "means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

In addition to the teachings regarding this claim element in LANProtect, MIMEsweeper discloses the storage of the corrupt mail messages or the data in removable area depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to perform one of the present actions recited by claim 18 as taught by LANProtect and MIMEsweeper in order to avoid downstream virus infection (not transmitting the data), provide the data to the intended destination (transmit unchanged) or perform traditional quarantining functionality (store the data in a file with a new name and notify the recipient). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper and the references applied against claim 18 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

MM. Whether claim 20 is unpatentable under 35 U.S.C. § 103 as being obvious over LANProtect, MIMEsweeper, Sidewinder, TIS Firewall and Layland, and further in view of SunScreen SPF-100

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the ‘600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the ‘600 patent. As shown above, no prior art concerning the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name was considered during prosecution of the ‘600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name raise a substantial new question of patentability with respect to claim 20 as pointed out in more detail below.

> **Claim 20** recites "The apparatus of claim 18, wherein the means for performing a preset action comprises:
>
> - means for transmitting the data unchanged;
> - means for not transmitting the data; and
> - means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 20 obvious.

This element is disclosed or suggested by a set of prior art including Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "SMTP `. *See e.g.*, TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.*, TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.*, Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 20. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages or the data according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the copying of the corrupt mail messages/data to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 20 obvious.

This element is disclosed or suggested by a set of prior art including Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). Sidewinder clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "SMTP`. *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.*, TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.*, Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 20. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 20 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify same to perform one of the present actions recited by claim 18 as taught by LANProtect and MIMEsweeper in order to avoid downstream virus infection (not transmitting the data), provide the data to the intended destination (transmit unchanged) or perform traditional quarantining functionality (store the data in a file with a new name and notify the recipient). Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 and the references applied against claim 18 are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

NN. Whether claim 21 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect

Claim 21 further adds the limitation to claim 18 of the subject patent that the apparatus is further capable of performing the steps for determining whether the data is of a type that is likely to contain a virus and capable of transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus. The steps of claim 21 are made obvious in view of the combination of the above-listed references as discussed below.

Claim 21: "The apparatus of claim 18 further comprising:"

(1) "…a second means for determining whether the data is of a type that is likely to contain a virus; and"

Claim 21 further recites "a second means for determining whether the data is of a type that is likely to contain a virus."

TFS Manual discloses this claim element. As discussed in TFS Manual, the TFS Gateway would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

In addition to the teachings relating to this element in TFS Manual, LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.* LANProtect at pg. 6 ("The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

(2) "…means for transmitting the data from the server to the destination without performing the steps of scanning,

determining, performing and sending, if the data is not of a type that is likely to contain a virus."

Claim 21 further recites "means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus."

TFS Manual discloses this claim element. If a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

In addition to the teachings relating to this element in TFS Manual, LANProtect discloses that this step is performed by the LANProtect product. When LANProtect is configured to scan only those file types likely to contain a virus, they do not scan at all other file types or take any of the preset actions.

Neither TFS Manual nor LANProtect were considered during prosecution of the '600 patent. These references contain a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.". As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* reexamination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the references applied to claim 18 to look at file extensions as taught by LANProtect and TFS Manual to allow configurability with respect to the types of files processed and/or to make virus scanning more efficient by avoiding scanning of those file types that are unlikely to contain a virus. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 18, LANProtect and TFS Manual are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

OO. Whether claim 21 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect, and further in view of Sidewinder

None of TFS Manual, LANProtect and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art that suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 21 as pointed out in more detail below.

Claim 21 recites "The apparatus of claim 18; further comprising:"

- a second means for determining whether the data is of a type that is likely to contain a virus; and
- means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus.

TFS Manual indicates that the TFS Gateway would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

In addition, TFS Manual discloses if a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

However the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." was somehow construed so that TFS Manual did not practice this aspect, the following references combined with TFS Manual would render claim 21 obvious.

This element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.* LANProtect at pg. 6 ("The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

LANProtect discloses that this step is performed by the LANProtect product. When LANProtect is configured to scan only those file types likely to contain a virus, they do not scan at all other file types or take any of the preset actions.

However the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 21 obvious.

This element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

None of TFS Manual, LANProtect and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the references applied to claim 18 to look at file extensions as taught by LANProtect, TFS Manual and Sidewinder to allow configurability with respect to the types of files processed and/or to make virus scanning more efficient by avoiding scanning of those file types that are unlikely to contain a virus. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 18, LANProtect, TFS Manual and Sidewinder are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

PP. Whether claim 22 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect and MIMEsweeper, and further in view of Cheswick and Bellovin

Claim 22 further adds the limitation to claim 18 of the subject patent that the apparatus further comprises of means for comparison of the destination address to valid addresses for the first network. The teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 22 of the '600 patent. The steps of claim 22 are obvious in view of the above-listed combination of references as discussed below.

Claim 22: "means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network"

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See e.g.,* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

In addition to the teachings relating to this element in TFS Manual, LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

In addition to the teachings relating to this element in TFS Manual and LANProtect, MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server involved receiving requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

In addition to the teachings relating to this element in TFS Manual, LANProtect and MIMEsweeper, Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the references applied to claim 18 to validate destination addresses as taught by LANProtect, TFS Manual, MIMEsweeper and Cheswick and Bellovin to allow the server to send the data to the client seeking to have the data sent to it. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 18, LANProtect, TFS Manual, MIMEsweeper and Cheswick and Bellovin are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

QQ. Whether claim 22 is unpatentable under 35 U.S.C. § 103 as being obvious over TFS Manual in view of LANProtect, MIMEsweeper, Cheswick and Bellovin and MpScan, and further in view of TIS Firewall

None of TFS Manual, LANProtect, MIMEsweeper, Cheswick and Bellovin, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the virus scanning apparatus further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the virus scanning apparatus comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first raise a substantial new question of patentability with respect to claim 12 as pointed out in more detail below.

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

In total, Claim 22 adds to claim 18 that the apparatus disclosed is further capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first.

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See e.g.,* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.")

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

LANProtect teaches receiving a data transfer request including a destination address. As LANProtect runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the data file.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server involved receiving requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41) ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS

Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

None of TFS Manual, LANProtect, MIMEsweeper, Cheswick and Bellovin, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 22 as pointed out above.

It would have been obvious to one of ordinary skill in the art at the time the alleged invention was made to modify the references applied to claim 18 to validate destination addresses as taught by LANProtect, TFS Manual, MIMEsweeper and Cheswick and Bellovin to allow the server to send the data to the client seeking to have the data sent to it. Meanwhile, as noted above KSR dictates the highly relevant and related teachings and technology relating to virus scanning and email processing in the references applied against claim 18, LANProtect, TFS Manual, MIMEsweeper and Cheswick and Bellovin are clearly properly combinable and representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of computer networks and email virus detection.

[* END OF REPLACEMENT SECTIONS ***]**

The Notice indicated the "explanation must not [] lump together the proposed rejections or proposed combinations of references." In this Replacement Statement and Explanation, the Requestor has now limited the explanations to the prior art combinations expressed by the substantial new questions (SNQs) of patentability identified at pages 2-7 (above); however, the Requestor does not admit or acknowledge that any of the SNQs represent the smallest combination of references sufficient to invalidate the claim or claims at issue. Rather, due to the vast amount of prior art available to call into question the validity of the '600 patent, for sake of keeping the number of substantial questions of patentability (SNQs) to a reasonable number, the Requestor has presented combinations of references that may be over inclusive. As such, in some cases, various subsets of the presented combinations of references are likely to be sufficient to invalidate the claims at issue and the Requestor invites the Examiner to make rejections based on such subsets.

The Request as now amended by this Replacement Statement and Explanation make clear that substantial new questions of patentability are raised in connection with claims 1-22 (all of the claims) of the '600 patent. In view of claims 1-22 of the '600 patent being rendered obvious in view of the previously cited and uncited prior art presented herein, it is respectfully requested that reexamination be granted and all claims of the '600 patent be cancelled as obvious.

The Requestor notes that since the filing of the Request the correspondence address of record for the '600 patent has changed to COVINGTON & BURLING, LLP, ATTN: PATENT DOCKETING, 1201 PENNSYLVANIA AVENUE, N.W., WASHINGTON DC 20004-2401. As such, a copy of the Request, in its entirety, as well as this Replacement Statement and Explanation are being served to this new correspondence address in accordance with 37 C.F.R. §§ 1.33(c) and 1.915(b)(6).

Please direct all correspondence to the undersigned.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date: July 21, 2010

By /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 064128
Ph: (303) 856-7155